BEST PRACTICES

July 12, 2005

Seven Habits Of Highly Effective Compliance Programs

by Michael Rasmussen

FORRESTER® Helping Business Thrive On Technology Change

July 12, 2005

Seven Habits Of Highly Effective Compliance Programs

by Michael Rasmussen
with Robert Markham, Laurie M. Orlov, Michael Hudson, and Samuel Bright

EXECUTIVE SUMMARY

Today, compliance is a daunting challenge to organizations because they are faced with a mountain of regulatory obligations. In the past, organizations tackled compliance as islands of projects scattered throughout the organization, leading to inconsistent approaches and a duplication of efforts. To achieve sustainable compliance, firms must develop a process and management function. In line with government guidance, sustainable compliance must encompass and sustain seven habits.

TABLE OF CONTENTS

NOTES & RESOURCES

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

"IT's Role In Enterprise Risk Management"
April 27, 2005, Trends

"IT Frameworks For Control And Compliance"
February 24, 2005, Best Practices

"Enterprise Risk Management"
December 29, 2004, Trends

"Trends 2005: Risk And Compliance Management"
October 25, 2004, Trends

"COSO Enterprise Risk Management Framework"
October 5, 2004, Quick Take

"Demystifying Compliance"
March 30, 2004, Trends

A PROCESS — NOT A PROJECT OR TECHNOLOGY

Regulatory compliance pressures plague organizations today — and there is no technology package that will provide the silver bullet to bring companies into compliance. Why? Business changes daily in size (e.g., employees, business partners, IT systems), products, and services, and firms often struggle to move from a regional to an international entity. Compliance is a bigger challenge than technology alone can solve, as:

- **Every part of the enterprise is affected.** Compliance challenges are broad and affect multiple parts of an enterprise and its partners. They include workforce and human resources regulations, environmental and public safety, corporate governance and ethics, sales practices, financial integrity and reporting, manufacturing, and the protection of personal information. Some compliance challenges span across industry verticals (e.g., Sarbanes-Oxley Act [SOX], Foreign Corrupt Practices Act, EU Data Protection), and many others are aimed at specific industries (e.g., TREAD Act, FDA 21 CFR Part 11, FDA GxMP).

- **Corporate governance is under the microscope.** Corporate disasters and growing government regulatory action heighten the focus on governance. Although compliance used to be handled in fragmented silos, the impact of risk and compliance on corporate governance is driving the centralization of compliance oversight within the organization. Compliance is now a defined function of enterprise risk management as a component of managing operational risk.[1]

Effective Compliance Programs Must Achieve Specific Goals

An organization that views compliance as individual project-management tasks across business units or groups is on a quick road to disaster. In reality, compliance is a process, not a project — requiring continuous oversight and ongoing management. In an effort to manage compliance and meet a multitude of compliance obligations, organizations are looking for a structured approach that allows them to identify and prioritize controls as well as establish a system of record.[2] Any effective compliance program must:[3]

- **Improve confidence — not just comply with regulation.** Increased control enables an organization to manage operational and financial integrity alongside compliance with laws and regulations, which increases confidence in business performance.[4]

- **Enhance visibility — not just meet requirements.** Increased control enhances the visibility, measurement, and management of operational risk as well as compliance, which allows an organization to understand where processes are breaking down.

- **Measure consistently — not just in disparate silos.** Consistency in terminology, measurement, risk, and controls allows for a systematic approach to compliance, which improves communication between compliance objectives and builds economies of scale.

SEVEN HABITS SUSTAIN A HIGHLY EFFECTIVE COMPLIANCE PROGRAM

As organizations react to the compliance burden and seek ways to leverage compliance to gain control and insight into the organization and enhance operational risk management, they are asking several important questions. What does a compliance management program look like? How do I incorporate compliance into the structure of the organization and respond to a dynamic business environment?

Understand The Regulatory Backdrop And Published Guidance

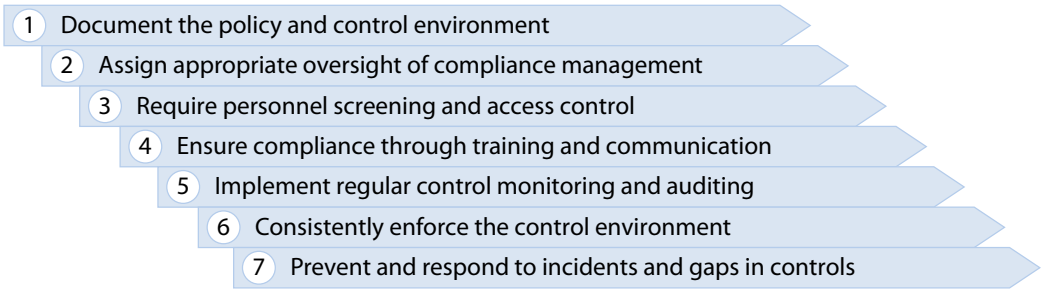
In 1991, the US Sentencing Commission (USSC) established the Organization Sentencing Guidelines to assist courts in determining due diligence versus negligence/culpability of organizations in matters of compliance. The USSC based its model on seven core elements for the courts to use in determining fines for organizations and sentences for executives in matters of criminal regulatory cases.[5]

- **The guidelines are now in effect . . .** The original USSC guidelines went into revision in 2001. These revisions went before Congress in April 2004, and it did not appeal the revisions. As a result, the revised and extended USSC Organization Sentencing Guidelines went into effect in November 2004. They were expressly expanded to include guidance for the courts in matters of SOX compliance and sentencing.

- **. . . and are applicable to all regulatory law.** The focus of the guidelines is on criminal regulatory conduct; however, the USSC has been explicit in its promotion of the guidelines in all matters of regulatory law.[6] The use of the USSC guidelines for all matters of regulatory law was well-established before this press release. Model guidance on compliance programs based on the USSC guidelines can be found through contacting the US Department of Justice, the US Environmental Protection Agency, the US Securities and Exchange Commission, the US Department of Labor's Occupational Safety & Health Administration, and the US Department of Health & Human Services.[7]

The USSC guidelines provide a commonsense framework around which organizations can structure their compliance management program. Using the USSC guidelines as a basis, Forrester has extended the seven elements to integrate research and experience on compliance best practices in large end user organizations — forming seven habits of a highly effective compliance program (see Figure 1).

Figure 1 Seven Habits Of A Highly Effective Compliance Program



Source: Forrester Research, Inc.

HABIT NO. 1: DOCUMENT THE POLICY AND CONTROL ENVIRONMENT

To demonstrate compliance, firms must start with how they document compliance and control architecture and explain this throughout the organization.

What Compliance And Control Documentation Should Cover

The overall architecture of compliance documentation is implemented through a control framework (e.g., COSO), and it documents policies, controls, standards, and procedures that align with compliance objectives and requirements.

- **Policy is the foundation for governance.** Policies must establish corporate governance, including the governance of compliance obligations. These policies establish the rules of expected behavior for individuals, business processes, technology, and business partner relationships. Adherence to policies allows individuals to perform their functions in a manner that illustrates compliance with the law and supports the organization's mission and strategic objectives.

- **Controls are the means to monitor compliance with policy.** Controls are the essential outcome of policies, procedures, and standards. Ultimately, controls are defined from policy statements and include the fine detail of the expectations and requirements established to meet compliance objectives.

- **Procedures and standards support policies.** Procedures and standards support policies and allow the organization to further manage corporate governance, risk, and compliance through prescribed objectives and steps.

Figure 2 Habit No. 1: Document The Policy And Control Environment

Source: Forrester Research, Inc.

The Characteristics Of Policy And Control Documentation

The policy and control architecture establishes the foundation for compliance upon which all the other seven habits are built. Without a proper governance model of policies and controls in place, it becomes impossible to oversee, communicate, monitor, enforce, or respond to gaps. It is the policy and control architecture for compliance that provides the framework for everything else to work within. This architecture is unique to each organization, reflecting its culture of control and industry requirements.

In developing and managing policy and control documentation, organizations must approach it through (see Figure 2):

- **Make documentation clearly written, relevant, and communicated.** Policies, procedures, standards, and supporting controls must be clearly written and relevant to the organization and its compliance/governance requirements. Policies, procedures, and standards must be available to those expected to comply with them.

- **Updating and maintaining documentation.** Management should review, maintain, and update policies, procedures, standards, and controls on a regular basis to ensure that they are relevant to corporate governance, operational control, and compliance. For example, one large financial services firm automatically triggers its policies into a review process every six months to ensure corporate relevancy. Outdated policies and controls establish obligations that can add unwarranted cost to the organization.

- **Using an operational control and compliance platform.** To manage the complexity of corporate policies and compliance controls, an organization should develop or purchase a platform to manage the development, maintenance, and communication of policies and documentation of controls. This tool should have a framework to manage operational risks, define policies and supporting controls to meet risks, conduct control self-assessments to validate control implementation and efficiency, and track control gaps and incidents in the environment.[8]

A Policy And Control Example: Mortgage Company

An international commercial mortgage company built an internal platform to manage operational risk, control, and compliance that spanned the operational risks and compliance obligations across the organization.

- **Scenario.** The firm defined 3,000 controls — 1,000 of these controls were specific to the IT environment — that spanned compliance requirements and supported corporate governance and policies. The platform is used to develop, maintain, and manage compliance and operational risk.

- **Benefit to the firm.** An architecture platform for operational risk and control to document compliance will identify the relationships of controls to policies, industry best practices/ guidance, and regulations. Controls can then be cross-referenced to the business assets (e.g. people, relationships, physical assets, information) they affect and the business processes they govern. Ultimately, metrics on operational and compliance control can be established for control validation and effectiveness through a dashboard and reporting. Organizations can then track incidents and losses back to controls and deficiencies and the assets and processes they affect.

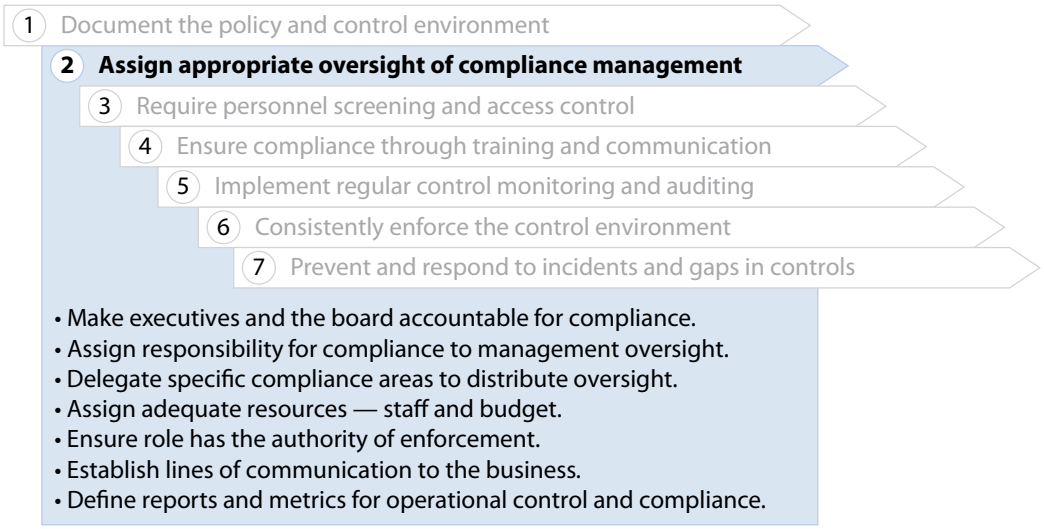
HABIT NO. 2: ASSIGN APPROPRIATE OVERSIGHT OF COMPLIANCE MANAGEMENT

The second habit of effective compliance is the establishment of appropriate oversight for compliance. A project approach for compliance could be disastrous — continuous business environment changes would mean that a new project would have to be launched. To keep abreast of business and IT changes, define compliance as a function with an individual ultimately accountable for compliance obligations.

The Breadth Of Oversight

In many organizations, the compliance role is siloed across different parts of the firm. One insurance mutual company houses the privacy and information compliance component within the IT department, while the controller's office oversees SOX compliance and a formal compliance office oversees the sales and ethics practices of the insurance products in all 50 US states. This results in substantial technology and effort duplication as well as a lack of visibility into compliance across the organization.

Figure 3 Habit No. 2: Assign Appropriate Oversight Of Compliance Management



Source: Forrester Research, Inc.

The Characteristics Of An Effective Oversight Model

Compliance oversight must achieve the mission and charter of the compliance program. Establishing the proper authority and governance of compliance is a critical requirement, followed by establishing the appropriate lines of communication to the extended business operational areas. The board and executive management must set this structure up with care and review it at least annually for effectiveness.

To be effective, organizations should develop a compliance oversight model that (see Figure 3):

- **Makes executives and the board accountable for compliance.** This is what is referred to as the "tone at the top." Ultimately, executive management and the board have the accountability and authority for compliance. They need to be knowledgeable about the content and operation of the compliance program. This tone shapes and develops the charter, structure, delegation of authority, and roles and responsibilities for the organization.

- **Assigns responsibility for compliance to management oversight.** The board must assign responsibility to an executive who is responsible for the overall operation of compliance across the organization. This individual may have the title of a chief risk officer (CRO) or a chief compliance officer (CCO). Depending on the organization's risk model, this may flow down to an individual who is responsible specifically for operational risk or compliance as part of operational risk. Some organizations refer to this role as an ethics officer. The size and industry of the organization will also alter how this role is defined.

- **Delegates specific compliance areas to distribute oversight.** Because large organizations carry a range of complex compliance obligations, it is difficult for one person to oversee all of them — it might be necessary to delegate responsibility to other individuals to manage specific sets of requirements and controls. This can take the form of direct reports to the CRO/CCO role or indirect reports to different areas of the organization directly affected by the compliance requirements faced.

- **Assigns adequate resources — staff and budget.** To manage compliance in the organization, the compliance officer role needs the resources to get the job done. This includes the appropriate staff and budget to maintain the compliance program.

- **Ensures that the role has the authority of enforcement.** Resources alone are not enough — the compliance role needs the appropriate authority to enable governance. This starts with a clearly defined charter and mission for the compliance function. To enable a compliance offer to succeed, the role must be assigned the autonomy to carry out the charter. When issues arise, the compliance officer needs direct access to executives, the board, and internal and external legal counsel.

- **Establishes lines of communication to the business.** To facilitate compliance, firms must establish a solid communication structure with affected business groups. The success of the compliance function depends on a good working relationship with critical business operations areas (e.g., internal audit, finance, legal). First, establish an active operational control and compliance committee that includes representatives of all functional business areas as well as executive management. Second, augment the committee with working groups that focus on specific compliance areas for planning and control development. In support of a centralized compliance role, many organizations today are also building supporting compliance roles within different business areas.

- **Defines reports and metrics for operational control and compliance.** Ultimately, the proper oversight of compliance includes the ability to report to executives, the board, and operational managers on the state of control and compliance within the organization and its extended business relationships.

An Effective Oversight Example: Consumer Banking

One consumer banking operation has established a role within IT aimed at IT risk and compliance management: the primary interaction point between IT and enterprise risk management. In other organizations, this person reports right into the operational risk officer below the CRO to separate the responsibilities from IT.

- **Scenario.** The bank's new role reports to the CIO and manages IT's risk and compliance obligations. The primary directive of this role is to manage risk and compliance in the following areas: IT architecture/standards, project, vendor/supplier, business continuity/disaster recovery, and information (e.g., personal information, intellectual property) risk and compliance. This individual fills the IT seat at the enterprise risk and compliance table, governed by the CRO.

- **Benefit.** The organization has clearly defined the lines of responsibility and reporting. Accountability remains at the board and executive levels, which have assigned a major role for compliance within the domain of operational risk under the CRO. Responsibility from there is further delegated down to the business area directly responsible for and most effective at meeting particular compliance requirements.

HABIT NO. 3: REQUIRE PERSONNEL SCREENING AND ACCESS CONTROL

The third habit of effective compliance is the assurance that the organization is not giving access to information and business processes to an individual likely to exhibit unethical behavior.

The Scope Of Personnel Screening And Access Control

Organizations must ensure through reasonable controls that they are not giving improper access to sensitive organization roles and information.

- **Initial background checks and screening.** The USSC guidelines call for background checks on high-level personnel before they are given access and responsibilities in the organization. Best practices in this area include the screening of all personnel with sensitive organizational access along with the assignment of appropriate access controls to sensitive processes and/or regulated organization information.

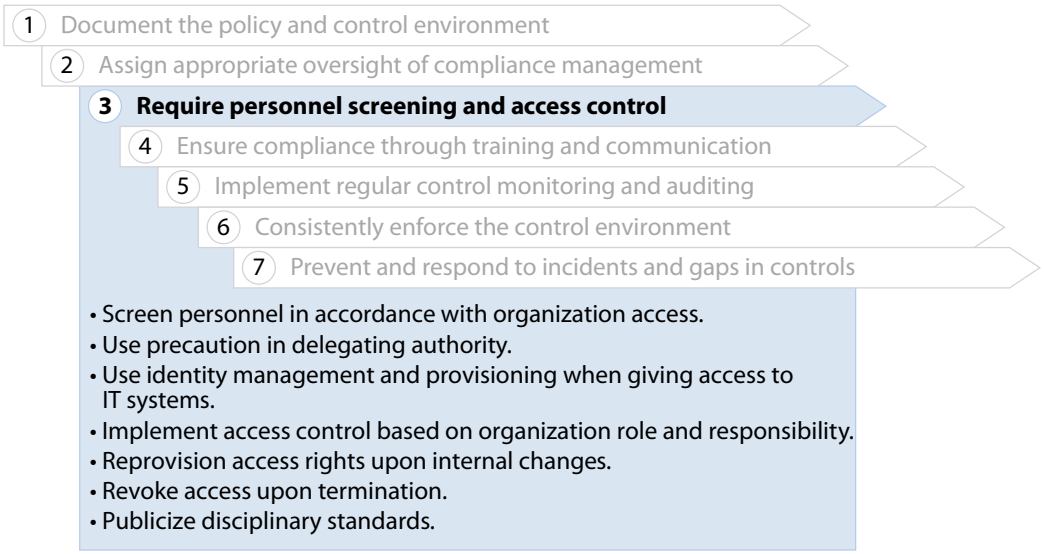
- **Ongoing regular reviews.** Employees and contractors must go through regular reviews and be checked routinely for a history of unethical behavior when they have access to sensitive information and processes. One of the greatest risks that organizations face within regulatory compliance is the internal threat from employees, contractors, and business partners.

The Characteristics Of Personnel And Access Control

A compliance officer is constantly thinking about who has access to sensitive, regulated processes and information. The wrong access given to regulated information can result in significant regulatory and financial penalties and a damaged reputation for an organization — and create extreme liabilities.

To ensure that appropriate and authorized access is available across the organization, organizations should (see Figure 4):

Figure 4 Habit No. 3: Require Personnel Screening And Access Control



Source: Forrester Research, Inc.

- **Screen personnel in accordance with organization access.** Before employees and contractors — as well as business partners — are allowed access to sensitive information, conduct a background check to make sure that they do not have a bent toward criminal behavior. The depth of the background check varies based on the level of access that the individual will have in the organization.

- **Use precaution in delegating authority.** Once a firm has screened personnel, it should take precautions to make sure they are not given more authority than they deserve for their position and that access is in line with the background information obtained. This also involves using care in the dissemination of regulated information to individuals within the organization and its extended relationships.

- **Use identity management and provisioning when giving access to IT systems.** Provisioning of users for internal systems that have sensitive and regulated information is best accomplished by provisioning access through a unique identification, such as a login ID. Digital information is only part of the problem; firms also need to pay close attention to regulated information no matter where it resides (e.g., oral communication, printed material, or what is held in an individual's memory).

- **Implement access control based on organization role and responsibility.** Access to information is best accomplished through centralized access-control mechanisms; in the IT world, this is done through role-based access control. Through access control, firms can regularly audit the separation of duties. Access to physical areas (e.g., records room, R&D, chemicals) must also be based on role and responsibility and then closely monitored.

- **Reprovision access rights upon internal changes.** Once an organization defines an employee's role and appropriate access, it needs to make sure to screen and provision rights again whenever the individual takes on a new role that interacts with sensitive and regulated processes and information. Without this safeguard, an individual could be hired and initially checked for criminal activity but then climb the corporate ladder to a role with access to controlled areas and avoid further background checks.

- **Revoke access upon termination.** Firms sometimes don't take action quickly enough upon voluntary or involuntary termination; instead, organizations should immediately revoke access to the technology and physical environments. This mitigates the risk of sabotage or unauthorized access following termination.

- **Publicize disciplinary standards.** To deter unlawful behavior around regulated information, disciplinary and monitoring standards must be well publicized in the organization. To further thwart unethical conduct, the organization should include the statement of how it will monitor activity with the disciplinary standards.

Learn From The Sad Tales Of Other Firms

The past six months have shown a wake of security incidents around personal financial information access: by fictitious business partners in the ChoicePoint breach and internal employees illegally selling personal information in the Wachovia/Bank of America breach. Consider the following two horror stories in which sensitive information was breached via:

- **A temporary employee.** One financial services firm learned the hard way that the internal threat to regulated information extends beyond information when a temporary worker hired for short-term staffing was given access to personal financial information and then stole customer identities. The organization is now examining how it can enforce and audit staffing agencies and require them to conduct background checks on temporary staff.

- **A business partner's employee.** A foreign national working for a large automanufacturer stole sensitive intellectual property through a business partner relationship. The company realized this theft occurred after a Chinese automanufacturer came out with a car with 80% of the same design specifications — and same malfunctions — as the one it was designing.

Effective Personnel Screening And Access Control Example: Consumer Banking

In response to the USSC requirements, one US financial services firm has established a process to prevent unauthorized access being granted to an individual before a background check is completed.

- **Scenario.** The IT department in this organization requires that HR acknowledge that a background check has been completed before it provisions a user on any internal IT system. Through the use of workflow, HR identifies the completion of a background check, which then assigns a task to IT to provision the identity with appropriate rights assigned to that role. Furthermore, internal changes trigger the IT department to revoke access to systems (the unique ID is maintained) and grant access in accordance with the individual's new role in the organization.

- **Benefit.** Through the enforcement of personnel screening, an organization can deter unethical behavior by hiring the right individuals. Furthermore, through the assignment and maintenance of appropriate access based on roles, the organization ensures that it is controlling and monitoring unwarranted access to regulated processes and information.

HABIT NO. 4: ENSURE COMPLIANCE THROUGH TRAINING AND COMMUNICATION

The fourth habit of effective compliance is the establishment of effective compliance awareness through active training and communication to internal employees, contractors, and business partners.

The Function Of A Compliance Training And Communication Program

To avoid corporate wrongdoing and fraud and reduce liability, organizations must implement effective compliance training programs to ensure compliance with regulations and corporate ethics.

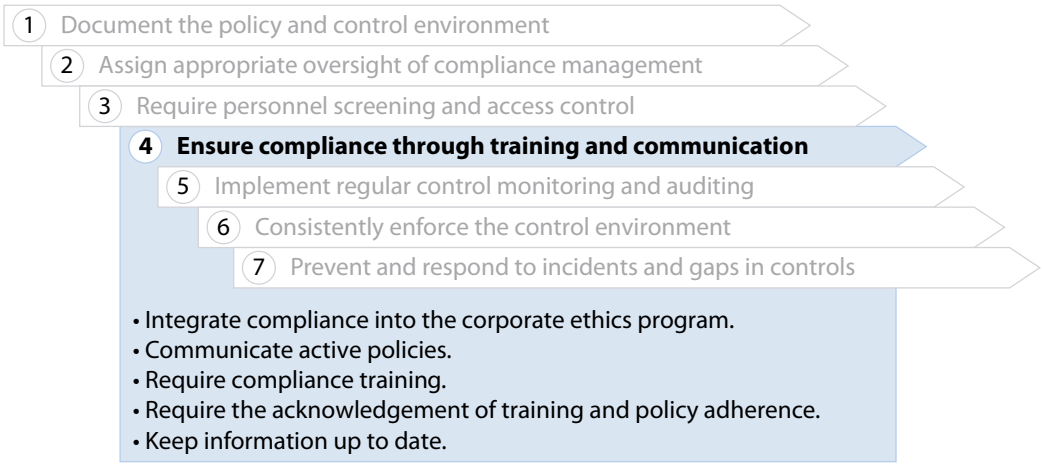
In the past, the USSC guidelines only required the communication of policies and procedures supporting compliance obligations. With the 2004 revisions, organizations now must document compliance communication and training programs; essentially, the organization has to ensure that individuals with access to regulated roles, processes, and information understand what they have to do to comply with the law and support corporate policy.

The Characteristics Of Compliance Training And Communication

Documented controls, oversight, and personnel screening and access controls are just the start of an effective compliance program. To effectively manage compliance, organizations need to validate that those in authority and with access to sensitive processes and information understand their compliance role and responsibility.

Characteristics of an effective compliance communication and training program include (see Figure 5):

Figure 5 Habit No. 4: Ensure Compliance Through Training And Communication



Source: Forrester Research, Inc.

- **The integration of compliance into the corporate ethics program.** Compliance obligations and requirements must be part of the corporate ethics program and supporting communication and training. As part of this, an organization must distribute all standards of conduct to all internal personnel who have access to regulated processes and information or have responsibilities that are regulated, such as board members, executives, managers, employees, and contractors. Business partners, while often overlooked, must also be included in the communication of ethics and standards of conduct enforced through contracts.

- **An active policy communication.** The organization must make corporate policies, procedures, and standards readily available and communicate them to personnel in positions with regulated access. Most organizations accomplish this through printed policy manuals as well as intranets. Alternative means of communicating policies, controls, ethics, and compliance include the use of newsletters, emails, posters, and announcements on computers screens.

- **Required compliance training.** The organization — through qualified trainers and curriculum — must conduct annual training for internal personnel, including contractors and consultants, who have access to regulated information and responsibilities. The compliance training program should be appropriate in length and frequency to keep fresh the ethics principles, policies, and controls required around regulated roles, practices, and information. Compliance training is broad and can be broken down into multiple areas covering topics like ethics, privacy, workforce safety, environmental safety, public safety, sales practices, and more. To facilitate training, organizations can take advantage of eLearning technologies, such as computer-based/ Web-based training.

- **The acknowledgement of training and policy adherence.** After reading policies and going through compliance training, the organization should require individuals to document their understanding and acknowledgement/adherence to corporate policies. Many organizations conduct online quizzing against policies and compliance obligations to document awareness. The organization should keep records of who has completed the required training, and it should impose sanctions for employees who fail to go through training and acknowledge policies.

- **Up-to-date information.** To remain effective, compliance training must be thorough and current by keeping abreast of relevant changes in regulations and case law. Evaluate the overall compliance training program on a regular basis to make sure it is consistent and sufficient to cover the latest requirements. Furthermore, firms must tailor compliance training to cover frequent compliance and policy violations — to increase awareness and reduce the risk of further violations.

Effective Compliance Training And Communication Example: Insurance/Mutual Company

In a leading insurance/mutual company, the USSC requirements for compliance training drove significant changes to the company's security awareness and compliance programs.

- **Scenario.** In the past, the company's program was highly focused on the awareness of security viruses and included content to make sure that employees did not open emails with attachments titled "I Love U." The awareness program is now focused on communicating privacy principles and policies that are in line with regulatory requirements that the company faces.

  In another part of the organization, the company uses compliance training and policy acknowledgement to document the field sales force's acceptance of regulations governing the sale of insurance products. Both areas of the organization are looking for ways to use technology to actively communicate compliance training, test user understanding of compliance obligations, and track policy acceptance.

- **Benefit.** By assigning staff to defined roles for awareness and training on compliance issues, the organization has been able to keep its program current and adapt to changing demands on the business. This has boosted the culture of compliance in the organization and allowed the organization to proceed with appropriate disciplinary actions when policies are violated — because these policies are actively acknowledged. Through the use of technology for eLearning and user testing, the organization hopes to deploy further automation and improve its communication of compliance requirements.

HABIT NO. 5: IMPLEMENT REGULAR CONTROL MONITORING AND AUDITING

The fifth habit for firms is the monitoring and auditing of control efficiency and effectiveness. Where the first habit focused on documenting controls, this habit focuses on the working operation of those controls.

Regular Control Monitoring And Auditing

A documented compliance program means nothing without implementation and sustained effectiveness of controls — in fact, it could open the doors of culpability and liability even wider when the organization documents policies and controls with which it does not comply. At that point, the organization has violated a responsibility that it has established for itself. The proper controls to monitor and audit vary in type.

- **Policy, operational, and technical controls.** Some controls are policy-based, such as written standards of expected behavior in an ethics policy. Others are operational in nature, such as describing procedures to be followed (e.g., aircraft maintenance logs), while others are technical in nature, such as system access monitoring, allowing for the automation of policy and operational controls.

- **Contractual controls.** There are contractual controls that transfer compliance obligations in business partner relationships — for example, the right to audit or confidentiality clauses.

- **Detective and preventive controls.** Controls are further broken down into detective controls, such as the review of transaction logs for inappropriate entries, that look for unethical behavior and preventive controls, such as controls enforcing the separation of duties on ERP systems, that prevent unethical behavior.

- **Compensating controls.** Compensating controls are established where it is difficult or impossible to implement preventive or detective controls into a system or process, such as compliance training, policy acknowledgement, and management oversight. They allow the organization to introduce controls outside of the process to compensate.

Firms should regularly monitor and audit controls through a manual or automated process that validates that the control is in place and operating effectively. Management must monitoring controls, while control auditing involves independent verification by an external or internal audit department about the state of control operation.

In ongoing control management, specifically on IT systems, many organizations are looking toward automated control monitoring and enforcement to ease the burden of control validation. An example is using control automation on ERP/financial systems for SOX compliance. Where controls cannot be automated, organizations should conduct control self-assessments that are facilitated through workflows on compliance management systems.

The Characteristics Of Control Monitoring And Auditing

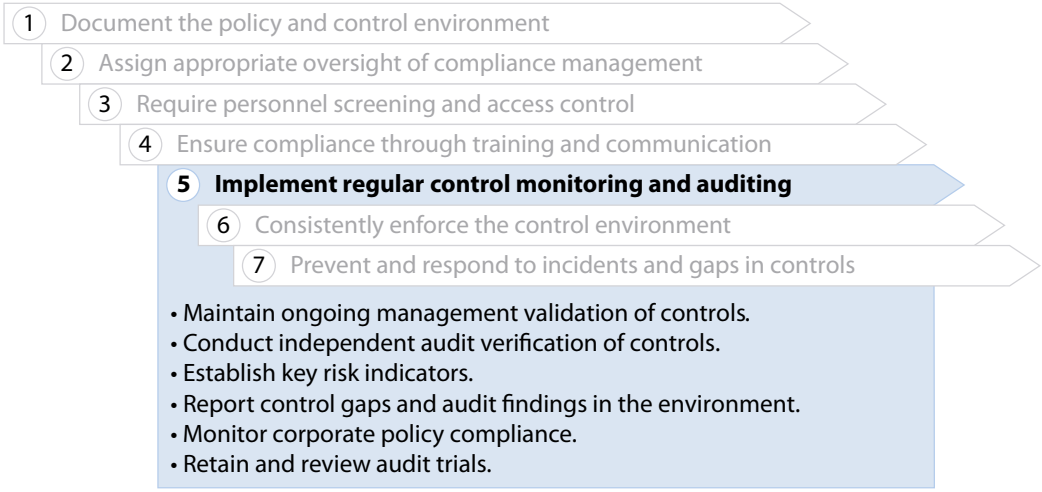
As stated, documented controls are meaningless and can only incur liability if they are not actually implemented and functioning in the environment. The role of compliance management is to implement a process of monitoring control implementation and effectiveness.

The critical factors in monitoring and auditing controls that an organization must have are (see Figure 6):

- **Ongoing management validation of controls.** The first step is regular control validation by management. This is conducted through automated control monitoring via technology or control self-assessments that are distributed to appropriate personnel to document the compliance, efficiency, and effectiveness of controls in the enterprise. The assurance of compliance involves the regular monitoring of controls by management in its defined role and oversight of business operations and relationships.

- **Independent audit verification of controls.** Internal and external audits have a role in compliance through the independent verification of controls in the audit process. The audit department should work with the compliance management function in conducting regularly scheduled audits, as well as be available for emergency situations caused by incidents or reports of gaps in controls. The role of the audit department is not to write controls — that is the job of compliance management and would be a conflict of interest — but to verify what compliance management has established.

Figure 6 Habit No. 5: Implement Regular Control Monitoring And Auditing



Source: Forrester Research, Inc.

- **The establishment of key risk indicators.** Along with control functions, the compliance function, as part of operational risk and control, must develop key indicators around critical operational and compliance risks. The goal is to alert the organization when a situation arises, a threshold is crossed, or a control has become deficient or nonexistent.

- **The reporting of control gaps and audit findings in the environment.** To facilitate control monitoring and further control development, all gaps and audit findings must be collected around operational and compliance risks. This, in turn, provides documentation of how the organization responds to breaches of compliance and deficiencies of controls. It also provides an historical record that can help the organization decide on further controls to prevent areas of significant gaps and business losses in the future.

- **The monitoring of corporate policy compliance.** The organization should exercise due care in enforcing policies consistently across the organization. Policy violation — particularly around regulated processes, roles, and information — should be part of performance reviews for employees and relationship/contract reviews with business partners.

- **The retention and review of audit trails.** As part of detective control, the organization should regularly review the audit trails of critical systems and processes for potential control violations, unethical conduct, and incidents. Additionally, audit trails should be archived to preserve evidence of what happened.

Effective Control Monitoring And Auditing Example: High-Tech Manufacturer

A high-tech manufacturer tackled SOX compliance — as well as management of operational risks — by building a framework and library of controls appropriate for the organization and working with, as opposed to against, its internal audit department.

- **Scenario.** The company began by documenting the control environment for its accounting systems and processes. It built a cooperative effort with its internal audit department to gain agreement on roles and controls for SOX compliance. It also built the control library on the COSO and COBIT frameworks, with management being responsible for the ongoing monitoring of controls and the audit department conducting an annual independent audit of controls. Management achieves ongoing monitoring through active control enforcement and monitoring in its SAP environment. It also conducts regular control self-assessments implemented through a software platform for SOX compliance with integrated workflow and content management.

- **Benefit.** Establishing a working relationship with the audit department that has clearly defined roles — as opposed to internal fighting over domains of responsibility — assisted the company in moving forward with SOX compliance. Furthermore, getting audit's input into the control framework and library upfront allows the organization to understand how audit will react to the

annual audit of controls. Using a compliance software platform for operational and compliance control provides economies of scale in the ongoing management and documentation of controls and assessments.

HABIT NO. 6: CONSISTENTLY ENFORCE THE CONTROL ENVIRONMENT

The sixth habit outlines how an effective compliance program ensures the consistent enforcement of policies and controls throughout the organization's environment and relationships.

The Goal Of Consistent Enforcement

Consistent enforcement of the control environment ensures that controls are applied appropriately across the organization and its business processes and relationships, guaranteeing that a specific individual's or business group's violations of controls or conduct are not ignored or overlooked but are enforced according to policy.

The organization's approach to ensuring consistent enforcement drives the success of the overall compliance program. It is through consistent enforcement that the organization's culture of compliance is achieved and that its employees understand that the organization has no tolerance for unethical and noncompliant conduct.

The Characteristics Of Consistent Enforcement Of The Control Environment

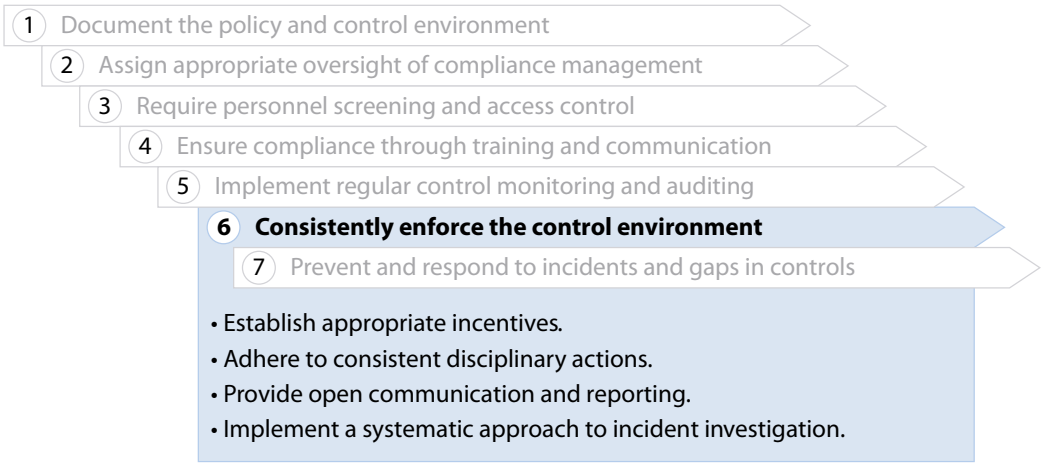
If management does not consistently enforce controls and discipline unethical and noncompliant behavior, the compliance program has failed. Penalties for noncompliance increase with regulators and the courts when organizations do not exhibit effective governance and enforcement practices.

Vital factors for consistent enforcement of the control environment include (see Figure 7):

- **Establishing appropriate incentives.** The organization must offer appropriate incentives to endorse strong ethical and compliance behavior. It should reward ethical conduct through performance reviews. This extends beyond just complying with requirements and includes rewarding those individuals who actively promote ethics and compliance through working with the organization to further control objectives and reporting.

- **Adhering to consistent disciplinary actions.** When an employee or contractor engages in unethical or noncompliant behavior, the organization must enforce consistent disciplinary actions. This includes discipline for failure to take reasonable steps to prevent such conduct. Rules without teeth have little effect on the organization; where positive incentives help foster a culture of compliance, consistent discipline drives it home.

Figure 7 Habit No. 6: Consistently Enforce The Control Environment



Source: Forrester Research, Inc.

- **Providing open communication and reporting.** The organization must establish an environment in which open communication and reporting of unethical and noncompliant conduct is possible without fear of retaliation. Regulatory guidance and the USSC guidelines require the establishment of incident reporting through whistleblower systems like anonymous Web and ethics telephone hot lines. The organization must publicize the whistleblower process well and make it available to all employees and contractors.

- **Implementing a systematic approach to incident investigation.** The organization must investigate all incidents of unethical and noncompliant behavior. It must protect itself by ensuring that incidents are not casually overlooked through the investigation of all potential incidents. Investigations that identify real incidents of wrongdoing must be documented and reported within the organization.

Effective Consistent Enforcement Example: Insurance Company

A large insurance company faced a dilemma: Information security was routinely appearing on noncompliance audit reports to the board of directors. The firm fixed the problem by tightening up the enforcement of policy and controls.

- **Scenario.** The board assigned management to remove information security from the audit report. Senior management at this insurance company tackled the challenge by hiring a chief information security officer (CISO). Over the next few years, the company went through two CISOs; both failed to get information security off the audit report. They were looking for technical ways to solve the problem. The third CISO decided that he was going to consistently

enforce policies and controls across the organization, establishing metrics that measured the consistency of policy and control enforcement.

- **Benefit.** Within one year of enforcing policies and controls, the objective was achieved: Information security was off the audit report. One intriguing metric tracked was how many people were fired in the past year for disciplinary actions concerning unethical behavior. In the first year, he measured more than 50 terminations; the next year it was down to fewer than 20. Corporate policies and compliance control enforcement are not optional; to work, they must have teeth.

HABIT NO. 7: PREVENT AND RESPOND TO INCIDENTS AND GAPS IN CONTROLS

An effective compliance program prevents and responds to compliance violations and gaps in controls and includes a lessons-learned process to prevent further violations.

Effective Prevention And Response To Incidents And Gaps In Controls

When a company identifies control deficiencies or incidents, it has to respond efficiently and effectively. Disregarding control gaps and compliance violations amounts to negligence — so do halfhearted attempts at a response. An effective compliance program must actively identify and close control gaps and contain or eliminate potential damage or loss to the organization incurred by violations. Control deficiencies and incident losses can be used for future control planning to maintain operational control, integrity, and effectiveness. This involves building a lessons-learned process when gaps and violations are identified.

The Characteristics Of Prevention And Response To Incidents And Control Gaps

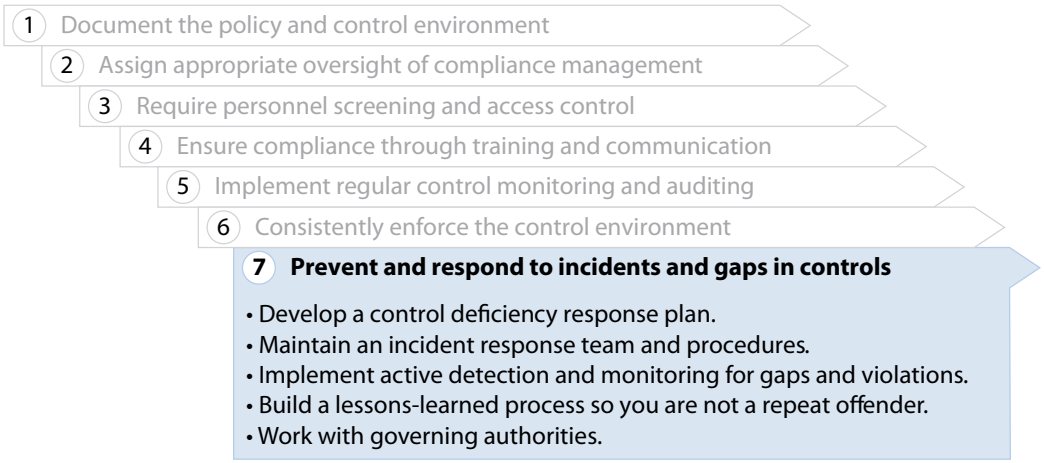
Deficiencies and gaps in controls will happen, as well as accidental or malicious violations of corporate policy and law. Courts and regulators recognize that bad things happen, but the final measure of culpability versus a demonstration of due diligence lies in the ability of the organization to respond to gaps and violations and prevent future infractions.

To complete an effective compliance program, the firm must (see Figure 8):

- **Develop a control deficiency response plan.** The first factor in an appropriate response to incidents and gaps in controls is to have a documented response plan. When the issue is a defined gap in controls, the organization should have a risk management process in place to determine the materiality of the control deficiency and aid in the evaluation of control selection.

- **Maintain an incident response team and procedures.** When the issue is an incident regarding unethical or noncompliant behavior, the organization should have an incident response plan in place to investigate the incident, contain the incident, collect evidence, and estimate damage. The response plan must contain response procedures and identify the appropriate response team members based on the type of incident.

Figure 8 Habit No. 7: Prevent And Respond To Incidents And Gaps In Controls



Source: Forrester Research, Inc.

- **Implement active detection and monitoring for gaps and violations.** To facilitate identifying control deficiencies/gaps and incidents, organizations should automate — where possible — the active detection and monitoring of controls. Detective controls are of particular interest; they alert the organization when behavior or attempted behavior is identified that violates policies and controls. The monitoring of audit trails is a primary example of active control and incident monitoring and detection.

- **Build a lessons-learned process so you are not a repeat offender.** The lessons-learned process is critical for organizations to fully comply with the USCC guidelines. The USSC guidelines are in place to determine sentences for compliance violators, and there are significant increases in sentences when the court finds that an organization is a repeat offender. To prevent future violations, an organization should develop corrective action plans that address incident findings and control deficiencies. It must also conduct regular reviews of repeated problem areas.

- **Work with governing authorities.** Another item weighed by the USSC guidelines is the extent that the organization has worked with governing authorities and regulators and law enforcement. As a best practice, organizations should build active and cooperative lines of communication with authorities and engage them according to response procedures and legal counsel review when incidents occur.

Effective Consistent Enforcement Example: Telecom Company

An international telecom company tackled response and prevention around compliance violations and control deficiencies by building a case/gap management system for compliance.

- **Scenario.** The firm's system provides a method for recording incidents and control deficiencies that the organization encountered while documenting response and losses incurred. This is part of the organization's efforts to manage operational risks and is used to track all operational incidents and losses in the enterprise as well as document deficiencies in controls and audit findings.

- **Benefit.** The case/gap management system provides a record of what happened and the impact on the organization, and it feeds back into further control analyses to optimize controls for preventing future incidents. This is accomplished through the collection of metrics to measure trends in losses and deficiencies for prioritizing future policies and controls.

RECOMMENDATIONS

COMPLIANCE INVOLVES POLICY, PEOPLE, PROCESS, AND TECHNOLOGY

When building a highly effective compliance program, keep in mind that all of the seven habits involve:

- **Policy.** Policies provide the governance for controls; it is through policies that expected ethical and compliant behavior is defined. While policies are part of the documentation in the first habit, they permeate all of the other habits, providing the behavioral foundation for each of them. Organizations must ensure that policies are well-defined and understood; without this effort, all else fails.
- **People.** Ultimately, compliance violations come down to people. Whether malicious or accidental, it is the people element that introduces uncertainty into the compliance process. Effective compliance program managers focus on developing a culture of compliance in which individuals behave ethically and responsibly.
- **Process.** Achieving effective compliance requires ongoing compliance processes. Organizations should avoid compliance islands and aim for consistency by approaching compliance as a process as opposed to individual projects.
- **Technology.** Technology is an important foundation for automating, consistency, and achieving economies of scale in compliance management. However, technology is not the complete answer — organizations must be wary of the multitude of "false prophet" technology vendors proclaiming the answer to all of your compliance needs. In fact, there is no single technology answer for compliance problems.

WHAT IT MEANS

ARCHITECT FOR SUSTAINABLE COMPLIANCE

Organizations that exhibit all seven habits make effective compliance a cost of being in business — not a one-time business event. For these firms, spending money on a compliance program averts far greater expense as a result of losses and penalties. They also establish greater operational control oversight, enabling them to pour more funding into expanding the business into new areas with confidence. These well-run companies will contrast sharply with those that remain reactive and tackle compliance problems as isolated and reactionary initiatives. The end game is a culture of compliance and controls; to paraphrase the USSC, an organizational culture that encourages a commitment to compliance with the law is one in which compliance with the law is expected behavior.[9]

ALTERNATIVE VIEW

WHY YOU CAN'T JUST SCRAPE BY

Organizations that do not embrace compliance management as a defined business process will approach compliance as fragmented projects, trying to sneak past the regulators' gaze. This minimalist mindset may appear to work for a short time; however, it is a recipe for disaster because no specific oversight compliance is in place. In today's dynamic business environment, gaps quickly arise that can push an organization out of compliance. IT systems, employees, relationships, and compliance requirements have changed; ultimately, business has changed. And no one has managed compliance accordingly. Furthermore, when regulators come asking questions and there is no central person ready to answer them, the organization looks confused and unorganized and will receive more scrutiny.

ENDNOTES

[1] The role of IT in enterprise risk management is twofold. First, IT has to manage risk and compliance within the IT department. Second, IT becomes an enabler for enterprise risk management by leveraging technology to proactively monitor and manage broader business risks and compliance. See the April 27, 2005, Trends "IT's Role In Enterprise Risk Management."

[2] Facing increased compliance obligations, a dynamic business and IT environment, fragmented risk and compliance projects, and exposure to tort and criminal liability, organizations are seeking a formalized approach to managing enterprise risk and compliance. See the October 25, 2004, Trends "Trends 2005: Risk And Compliance Management."

[3] Departing SEC chairman William Donaldson drives home the need for an effective compliance program in the following point: "Successful corporate leaders must therefore strive to do the right thing, in disclosure, in governance and otherwise in their businesses. And they must instill in their corporations this attitude of doing the right thing. Simply complying with the rules is not enough. They should, as I have said before, make this approach part of their companies' DNA. For companies that take this approach, most of the major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities — opportunities to improve internal controls, improve the performance of the board, and improve their public reporting — they will ultimately be better run, more transparent, and therefore more attractive to investors." Source: Chairman William H. Donaldson, "Speech by SEC Chairman: Remarks to the National Press Club," Washington, D.C., July 30, 2003 (http://www.sec.gov/news/speech/spch073003whd.htm).

[4] Financial integrity, operational integrity, and regulatory/legal compliance are the three primary objectives of the Committee of Sponsoring Organizations' (COSO) Internal Control Framework. This is the most common framework being used for compliance today.

[5] The USSC guidelines can be found on the USSC site at http://www.ussc.gov.

[6] In a press release issued on May 3, 2004, the USSC stated: "An effective compliance program has been a fundamental component of the organizational sentencing guidelines since the Commission first promulgated them in 1991. Under the guidelines, an organization's punishment is adjusted according to several factors, one of which is whether the organization has in place an effective program to prevent and detect violations of law. For such a program to be considered effective, the Commission articulated seven minimum requirements. In 1991, these seven requirements represented the federal government's first attempt to articulate such broad-based standards, and they quickly became the benchmark against which most organizations measured their compliance programs." Source: "Commission Tightens Requirements For Corporate Compliance And Ethics Programs," USSC press release, May 3, 2004 (http://www.ussc.gov/PRESS/rel0504.htm).

[7] Regulator guidance on "effective compliance programs" built on the USSC Organizational Sentencing Guidelines model are illustrated by the standards created by the Department of Health & Human Services (e.g., 64 Federal Register 36368 [July 9, 1999]). The following links provide more information on HHS guidance on compliance that mirrors that of the USSC: http://oig.hhs.gov/authorities/frnotices.html, http://oig.hhs.gov/fraud/docs/complianceguidance/012705HospSupplementalGuidance.pdf, and http://oig.hhs.gov/authorities/docs/03/050503FRCPGPharmac.pdf.

[8] Common operational control and compliance software vendors that support platform-spanning business regulations include Axentis, IBM, OpenPages, Paisley Consulting, and Qumas. Archer Technologies supports information risk and compliance regulations.

[9] Source: "Sentencing Commission Toughens Requirements For Corporate Compliance And Ethics Programs," USSC press release, April 13, 2004 (http://www.ussc.gov/PRESS/rel0404.htm).

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia
Brazil
Canada
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Sweden
Switzerland
United Kingdom
United States

For a complete list of worldwide locations, visit www.forrester.com/about.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®